Chaotic Iterations for Steganography - Stego-security and chaos-security

Nicolas Friot, Christophe Guyeux, Jacques Bahi

CHAOTIC ITERATIONS FOR STEGANOGRAPHY
Stego-security and topological-security

Nicolas Friot, Christophe Guyeux, and Jacques M. Bahi

Computer Science Laboratory LIFC
University of Franche-Comté
16 route de Gray, Besançon, France

{nicolas.friot, christophe.guyeux, jacques.bahi}@lifc.univ-fcomte.fr

December 16, 2011

Keywords: Steganography; Topology; Security; Information hiding; Stego-security; Topological-security; Chaotic Iterations.

Abstract

In this paper is proposed a novel steganographic scheme based on chaotic iterations. This research work takes place into the information hiding security fields. We show that the proposed scheme is stego-secure, which is the highest level of security in a well defined and studied category of attack called "watermark-only attack". Additionally, we prove that this scheme presents topological properties so that it is one of the firsts able to face, at least partially, an adversary when considering the others categories of attacks defined in the literature.

1 Introduction

Robustness and security are two major concerns in information hiding [17, 13]. These two concerns have been defined in [16] as follows. "Robust watermarking is a mechanism to create a communication channel that is multiplexed into original content [...]. It is required that, firstly, the perceptual degradation of the marked content [...] is minimal and, secondly, that the capacity of the watermark channel degrades as a smooth function of the degradation of the marked content. [...]. Watermarking security refers to the inability by unauthorized users to have access to the raw watermarking channel. [...] to remove, detect and estimate, write or modify the raw watermarking bits." We will focus in this research work on security.

In the framework of watermarking and steganography, security has seen several important developments since the last decade [5, 11, 18, 7]. The first fundamental work in security was made by Cachin in the context of steganography [8]. Cachin interprets the attempts of an attacker to distinguish between an innocent image and a stego-content as a hypothesis testing problem. In this document, the basic properties of a stegosystem are defined using the notions of entropy, mutual information, and relative entropy. Mittelholzer, inspired by the work of Cachin, proposed the first theoretical framework for analyzing the security of a watermarking scheme [19].

These efforts to bring a theoretical framework for security in steganography and watermarking have been followed up by Kalker, who tries to clarify the concepts (robustness *vs.* security), and the classifications of watermarking attacks [16]. This work has been deepened by Furon *et al.*, who have translated Kerckhoffs' principle (Alice and Bob shall only rely on some previously shared secret for privacy), from cryptography to data hiding [14]. They used Diffie and Hellman methodology, and Shannon's cryptographic framework [21], to classify the watermarking attacks into categories,

according to the type of information Eve has access to [11, 20], namely: Watermarked Only Attack (WOA), Known Message Attack (KMA), Known Original Attack (KOA), and Constant-Message Attack (CMA). Levels of security have been recently defined in these setups. The highest level of security in WOA is called stego-security [10], whereas topological-security tends to improve the ability to withstand attacks in KMA, KOA, and CMA setups [15].

To the best of our knowledge, there exist only two information hiding schemes that are both stego-secure and topologically-secure [15]. The first one is based on a spread spectrum technique called Natural Watermarking. It is stego-secure when its parameter η is equal to 1 [10]. Unfortunately, this scheme is neither robust, nor able to face an attacker in KOA and KMA setups, due to its lack of a topological property called expansivity [15]. The second scheme both topologically-secure and stego-secure is based on chaotic iterations [2]. However, it allows to embed securely only one bit per embedding parameters. The objective of this research work is to improve the scheme presented by authors of [2], in such a way that more than one bit can be embedded.

The remainder of this document is organized as follows. In Section 2, some basic recalls concerning both chaotic iterations and Devaney's chaos are given. In Section 3 are presented results and information hiding scheme on which our work is based. Classes of attacks considered in this paper are detailed in Section 4. Stego-security and topological-security are recalled too in this section. The new information hiding scheme is given in Section 5. Its stego-security is studied in the next section. The topological framework making it possible to evaluate topological-security is introduced in Section 7. Then the topological properties of our scheme are investigated in the next section, leading to the evaluation of its topological-security. This research work ends by a conclusion section where our contribution is summarized and intended future researches are presented.

2 Basic Recalls

2.1 Chaotic Iterations

In the sequel S^n denotes the n^{th} term of a sequence S and V_i is for the i^{th} component of a vector V. Finally, the following notation is used: $[\![0;N]\!] = \{0,1,\ldots,N\}$.

Let us consider a *system* of a finite number N of elements (or *cells*), so that each cell has a boolean *state*. A sequence of length N of boolean states of the cells corresponds to a particular *state of the system*. A sequence that elements belong into $[\![0;\mathsf{N}-1]\!]$ is called a *strategy*. The set of all strategies is denoted by $\mathbb{S}$.

Definition 1. *The set* $\mathbb{B}$ *denoting* $\{0,1\}$*, let* $f : \mathbb{B}^{\mathsf{N}} \longrightarrow \mathbb{B}^{\mathsf{N}}$ *be a function and* $S \in \mathbb{S}$ *be a strategy. The so-called* chaotic iterations *are defined by* $x^0 \in \mathbb{B}^{\mathsf{N}}$ *and* $\forall (n,i) \in \mathbb{N}^* \times [\![0;\mathsf{N}-1]\!]$*:*

$$x_i^n = \begin{cases} x_i^{n-1} & \text{if } S^n \neq i, \\ \left(f(x^{n-1})\right)_{S^n} & \text{if } S^n = i. \end{cases}$$

2.2 Devaney's Chaotic Dynamical Systems

Some topological definitions and properties taken from the mathematical theory of chaos are recalled in this section.

Let $(\mathcal{X},d)$ be a metric space and f a continuous function on $(\mathcal{X},d)$.

Definition 2. f *is said to be* topologically transitive *if, for any pair of open sets* $U,V \subset \mathcal{X}$*, there exists* $k > 0$ *such that* $f^k(U) \cap V \neq \varnothing$.

Definition 3. $(\mathcal{X}, f)$ *is said to be* regular *if the set of periodic points is dense in* $\mathcal{X}$.

Definition 4. f *has* sensitive dependence on initial conditions *if there exists* $\delta > 0$ *such that, for any* $x \in \mathcal{X}$ *and any neighborhood* V *of* x*, there exist* $y \in V$ *and* $n \geqslant 0$ *such that* $d\left(f^n(x), f^n(y)\right) > \delta$.

δ *is called the* constant of sensitivity *of* f.

It is now possible to introduce the well-established mathematical definition of chaos [12],

Definition 5. *A function* $f : \mathcal{X} \longrightarrow \mathcal{X}$ *is said to be* chaotic *on* $\mathcal{X}$ *if:*

1. *f is regular,*
2. *f is topologically transitive,*
3. *f has sensitive dependence on initial conditions.*

When f is chaotic, then the system $(\mathcal{X}, f)$ is chaotic and quoting Devaney: "it is unpredictable because of the sensitive dependence on initial conditions. It cannot be broken down or simplified into two subsystems which do not interact because of topological transitivity. And in the midst of this random behavior, we nevertheless have an element of regularity". Fundamentally different behaviors are consequently possible and occur in an unpredictable way.

Let us finally remark that,

Theorem 1 ([4])**.** *If a function is regular and topologicaly transitive on a metric space, then the function is sensitive on initial conditions.*

3 Information hiding based on chaotic iterations

3.1 Topology of Chaotic Iterations

In this section, we give the outline proofs establishing the topological properties of chaotic iterations. As our scheme is inspired by the work of Guyeux *et al.* [15, 2, 1], the proofs detailed at the end of this document will follow a same canvas.

Let us firstly introduce some notations and terminologies.

Definition 6. *Let* $\mathsf{k} \in \mathbb{N}^*$*. A* strategy adapter *is a sequence which elements belong into* $[\![0, \mathsf{k}-1]\!]$*. The set of all strategies with terms in* $[\![0, \mathsf{k}-1]\!]$ *is denoted by* $\mathbb{S}_\mathsf{k}$*.*

Definition 7. *The* discrete boolean metric *is the application* $\delta : \mathbb{B} \longrightarrow \mathbb{B}$ *defined by* $\delta(x,y) = 0 \Leftrightarrow x = y$*.*

Definition 8. *Let* $k \in \mathbb{N}^*$*. The* initial function *is the map* i_k *defined by:*

$$\begin{array}{rccc} i_k : & \mathbb{S}_k & \longrightarrow & [\![0, \mathsf{k}-1]\!] \\ & (S^n)_{n\in\mathbb{N}} & \longmapsto & S^0 \end{array}$$

Definition 9. *Let* $k \in \mathbb{N}^*$*. The* shift function *is the map* σ_k *defined by:*

$$\begin{array}{rccc} \sigma_k : & \mathbb{S}_k & \longrightarrow & \mathbb{S}_k \\ & (S^n)_{n\in\mathbb{N}} & \longmapsto & (S^{n+1})_{n\in\mathbb{N}} \end{array}$$

Definition 10. *Given a function* $f : \mathbb{B}^\mathsf{N} \to \mathbb{B}^\mathsf{N}$*, the function* F_f *is defined by:*

$$\begin{array}{rl} F_f : & [\![0; \mathsf{N}-1]\!] \times \mathbb{B}^\mathsf{N} \longrightarrow \mathbb{B}^\mathsf{N} \\ & (k,E) \longmapsto \left(E_j.\delta(k,j) + f(E)_k.\overline{\delta(k,j)}\right)_{j\in[\![0;\mathsf{N}-1]\!]} \end{array}$$

Definition 11. *The phase space used for chaotic iterations is denoted by* $\mathcal{X}_1$ *and defined by* $\mathcal{X}_1 = \mathbb{S}_\mathsf{N} \times \mathbb{B}^\mathsf{N}$*.*

Definition 12. *Given a function* $f : \mathbb{B}^\mathsf{N} \to \mathbb{B}^\mathsf{N}$*, the map* G_f *is defined by:*

$$\begin{array}{rccc} G_f : & \mathcal{X}_1 & \longrightarrow & \mathcal{X}_1 \\ & (S,E) & \longmapsto & (\sigma_\mathsf{N}(S), F_f(i_\mathsf{N}(S),E)) \end{array}$$

With these definitions, chaotic iterations can be described by the following iterations of the discret dynamical system:

$$\left\{ \begin{array}{l} X^0 \in \mathcal{X}_1 \\ \forall k \in \mathbb{N}^*, X^{k+1} = G_f(X^k) \end{array} \right.$$

Finally, a new distance d_1 between two points has been defined by:

Definition 13 (Distance d_1 on $\mathcal{X}_1$)**.** $\forall (S,E),(\check{S},\check{E}) \in \mathcal{X}_1$, $d_1((S,E);(\check{S},\check{E})) = d_{\mathbb{B}^{\mathsf{N}}}(E,\check{E}) + d_{\mathbb{S}_{\mathsf{N}}}(S,\check{S})$, *where:*

- $d_{\mathbb{B}^{\mathsf{N}}}(E,\check{E}) = \sum_{k=0}^{\mathsf{N}-1} \delta(E_k,\check{E}_k) \in [\![0;\mathsf{N}]\!]$
- $d_{\mathbb{S}_{\mathsf{N}}}(S,\check{S}) = \frac{9}{\mathsf{N}} \sum_{k=1}^{\infty} \frac{|S^k - \check{S}^k|}{10^k} \in [0;1]$.

are respectively two distances on $\mathbb{B}^{\mathsf{N}}$ *and* $\mathbb{S}_{\mathsf{N}}$ *(*$\forall \mathsf{N} \in \mathbb{N}^*$*).*

Remark 1. *This new distance has been introduced by authors of [1] to satisfy the following requirements. When the number of different cells between two systems is increasing, then their distance should increase too. In addition, if two systems present the same cells and their respective strategies start with the same terms, then the distance between these two points must be small, because the evolution of the two systems will be the same for a while. The distance presented above follows these recommendations.*

It is then proven that,

Proposition 1. *G_f is a continuous function on $(\mathcal{X}_1,d_1)$, for all $f : \mathbb{B}^{\mathsf{N}} \to \mathbb{B}^{\mathsf{N}}$.*

Let us now recall the iteration function used by authors of [2].

Definition 14. *The* vectorial negation *is the function defined by:*

$$\begin{array}{rccc} f_0 : & \mathbb{B}^{\mathsf{N}} & \longrightarrow & \mathbb{B}^{\mathsf{N}} \\ & (b_0,\cdots,b_{\mathsf{N}-1}) & \longmapsto & (\overline{b_0},\cdots,\overline{b_{\mathsf{N}-1}}) \end{array}$$

In the metric space $(\mathcal{X}_1,d_1)$, G_{f_0} satisfies the three conditions for Devaney's chaos: regularity, transitivity, and sensitivity. So,

Theorem 2. *G_{f_0} is a chaotic map on $(\mathcal{X}_1,d_1)$ according to Devaney.*

Finally, it has been stated in [1] that,

Proposition 2. *The phase space $\mathcal{X}_1$ has, at least, the cardinality of the continuum.*

3.2 Chaotic Iterations for Data Hiding

To explain how to use chaotic iterations for information hiding, we must firstly define the significance of a given coefficient.

3.2.1 Most and Least Significant Coefficients

We first notice that terms of the original content *x* that may be replaced by terms issued from the watermark *y* are less important than other: they could be changed without be perceived as such. More generally, a *signification function* attaches a weight to each term defining a digital media, depending on its position *t*.

Definition 15. *A* signification function *is a real sequence* $(u^k)^{k\in\mathbb{N}}$.

Example 1. *Let us consider a set of grayscale images stored into portable graymap format (P3-PGM): each pixel ranges between 256 gray levels, i.e., is memorized with eight bits. In that context, we consider* $u^k = 8 - (k \mod 8)$ *to be the k-th term of a signification function* $(u^k)^{k\in\mathbb{N}}$*. Intuitively, in each group of eight bits (i.e., for each pixel) the first bit has an importance equal to 8, whereas the last bit has an importance equal to 1. This is compliant with the idea that changing the first bit affects more the image than changing the last one.*

Definition 16. *Let* $(u^k)^{k\in\mathbb{N}}$ *be a signification function, m and M be two reals s.t.* $m < M$.

- *The* most significant coefficients (MSCs) *of x is the finite vector*

$$u_M = \left(k \;\middle|\; k \in \mathbb{N} \text{ and } u^k \geqslant M \text{ and } k \leq |\, x \,|\right);$$

- *The* least significant coefficients (LSCs) *of x is the finite vector*

$$u_m = \left(k \mid k \in \mathbb{N} \text{ and } u^k \leq m \text{ and } k \leq |\, x \,|\right);$$

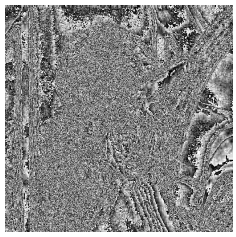
- *The* passive coefficients *of x is the finite vector*

$$u_p = \left(k \mid k \in \mathbb{N} \text{ and } u^k \in]m; M[\text{ and } k \leq |\, x \,|\right).$$

For a given host content x, MSCs are then ranks of x that describe the relevant part of the image, whereas LSCs translate its less significant parts. These two definitions are illustrated on Figure 1, where the significance function (u^k) is defined as in Example 1, $M = 5$, and $m = 6$.

(a) Original Lena.

(b) MSCs of Lena.



(c) LSCs of Lena ($\times 17$).

Figure 1: Most and least significant coefficients of Lena.

3.2.2 Presentation of the Scheme

Authors of [2] have proposed to use chaotic iterations as an information hiding scheme, as follows. Let:

- $(K, N) \in [0;1] \times \mathbb{N}$ be an embedding key,
- $X \in \mathbb{B}^{\mathsf{N}}$ be the N LSCs of a cover C,
- $(S^n)_{n\in\mathbb{N}} \in [\![0, \mathsf{N}-1]\!]^{\mathbb{N}}$ be a strategy, which depends on the message to hide $M \in [0;1]$ and K,
- $f_0 : \mathbb{B}^{\mathsf{N}} \to \mathbb{B}^{\mathsf{N}}$ be the vectorial logical negation.

So the watermarked media is C whose LSCs are replaced by $Y_K = X^N$, where:

$$\begin{cases} X^0 = X \\ \forall n < N, X^{n+1} = G_{f_0}(X^n). \end{cases}$$

Two ways to generate $(S^n)_{n\in\mathbb{N}}$ are given by these authors, namely Chaotic Iterations with Independent Strategy (CIIS) and Chaotic Iterations with Dependent Strategy (CIDS). In CIIS, the strategy is independent from the cover media C, whereas in CIDS the strategy will be dependent on C. As we will use the CIIS strategy in this document, we recall it below. Finally, MSCs are not used here, as we do not consider the case of authenticated watermarking.

3.2.3 CIIS Strategy

Let us firstly give the definition of the Piecewise Linear Chaotic Map (PLCM, see [22]):

$$F(x,p) = \begin{cases} x/p & \text{if} \quad x \in [0;p], \\ (x-p)/(\frac{1}{2}-p) & \text{if} \quad x \in \left[p;\frac{1}{2}\right], \\ F(1-x,p) & \text{else,} \end{cases}$$

where $p \in \left]0;\frac{1}{2}\right[$ is a "control parameter".

Then, the general term of the strategy $(S^n)_n$ in CIIS setup is defined by the following expression: $S^n = \lfloor \mathsf{N} \times K^n \rfloor + 1$, where:

$$\begin{cases} p \in \left[0; \frac{1}{2}\right] \\ K^0 = M \otimes K \\ K^{n+1} = F(K^n, p), \forall n \leq N_0 \end{cases}$$

in which $\otimes$ denotes the bitwise exclusive or (XOR) between two floating part numbers (*i.e.*, between their binary digits representation).

4 Data hiding security

4.1 Classification of Attacks

In the steganography framework, attacks have been classified in [10] as follows.

Definition 17. *Watermark-Only Attack (WOA) occurs when an attacker has only access to several watermarked contents.*

Definition 18. *Known-Message Attack (KMA) occurs when an attacker has access to several pairs of watermarked contents and corresponding hidden messages.*

Definition 19. *Known-Original Attack (KOA) is when an attacker has access to several pairs of watermarked contents and their corresponding original versions.*

Definition 20. *Constant-Message Attack (CMA) occurs when the attacker observes several watermarked contents and only knows that the unknown hidden message is the same in all contents.*

4.2 Stego-Security

In the prisoner problem of Simmons [23, 6], Alice and Bob are in jail, and they want to, possibly, devise an escape plan by exchanging hidden messages in innocent-looking cover contents. These messages are to be conveyed to one another by a common warden, Eve, who over-drops all contents and can choose to interrupt the communication if they appear to be stego-contents.

The stego-security, defined in this framework, is the highest security level in WOA setup [10]. To recall it, we need the following notations:

- $\mathbb{K}$ is the set of embedding keys,
- $p(X)$ is the probabilistic model of N_0 initial host contents,
- $p(Y|K_1)$ is the probabilistic model of N_0 watermarked contents.

Furthermore, it is supposed in this context that each host content has been watermarked with the same secret key K_1 and the same embedding function e.

It is now possible to define the notion of stego-security:

Definition 21 (Stego-Security)**.** *The embedding function e is* stego-secure *if and only if:*

$$\forall K_1 \in \mathbb{K}, p(Y|K_1) = p(X).$$

To the best of our knowledge, until now, only two schemes have been proven to be stego-secure. On the one hand, the authors of [10] have established that the spread spectrum technique called Natural Watermarking is stego-secure when its distortion parameter η is equal to 1. On the other hand, it has been proven in [15] that:

Proposition 3. *Chaotic Iterations with Independent Strategy (CIIS) are stego-secure.*

4.3 Topological-Security

To check whether an information hiding scheme S is topologically-secure or not, S must be written as an iterate process $x^{n+1} = f(x^n)$ on a metric space $(\mathcal{X}, d)$. This formulation is always possible [3]. So,

Definition 22 (Topological-Security)**.** *An information hiding scheme S is said to be topologically-secure on* $(\mathcal{X},d)$ *if its iterative process has a chaotic behavior according to Devaney.*

In the approach presented by Guyeux *et al.*, a data hiding scheme is secure if it is unpredictable. Its iterative process must satisfy the Devaney's chaos property and its level of topological-security increases with the number of chaotic properties satisfied by it.

This new concept of security for data hiding schemes has been proposed in [3] as a complementary approach to the existing framework. It contributes to the reinforcement of confidence into existing secure data hiding schemes. Additionally, the study of security in KMA, KOA, and CMA setups is realizable in this context. Finally, this framework can replace stego-security in situations that are not encompassed by it. In particular, this framework is more relevant to give evaluation of data hiding schemes claimed as chaotic.

5 The improved algorithm

In this section is introduced a new algorithm that generalize the scheme presented by authors of [2].

Let us firstly introduce the following notations:

- $x^0 \in \mathbb{B}^{\mathsf{N}}$ is the N least significant coefficients of a given cover media C.
- $m^0 \in \mathbb{B}^{\mathsf{P}}$ is the watermark to embed into x^0.
- $S_p \in \mathbb{S}_N$ is a strategy called **place strategy**.
- $S_c \in \mathbb{S}_P$ is a strategy called **choice strategy**.
- Lastly, $S_m \in \mathbb{S}_P$ is a strategy called **mixing strategy**.

Our information hiding scheme called Steganography by Chaotic Iterations and Substitution with Mixing Message (SCISMM) is defined by $\forall (n,i,j) \in \mathbb{N}^* \times [\![0;\mathsf{N}-1]\!] \times [\![0;\mathsf{P}-1]\!]$:

$$\begin{cases} x_i^n = \begin{cases} x_i^{n-1} & \text{if } S_p^n \neq i \\ m_{S_c^n} & \text{if } S_p^n = i. \end{cases} \\ \\ m_j^n = \begin{cases} m_j^{n-1} & \text{if } S_m^n \neq j \\ \\ \overline{m_j^{n-1}} & \text{if } S_m^n = j. \end{cases} \end{cases}$$

where $\overline{m_j^{n-1}}$ is the boolean negation of m_j^{n-1}.

The stego-content is the boolean vector $y = x^P \in \mathbb{B}^{\mathsf{N}}$.

6 Study of stego-security

Let us prove that,

Proposition 4. *SCISMM is stego-secure.*

Proof. Let us suppose that $x^0 \sim \mathbf{U}\left(\mathbb{B}^N\right)$ and $m^0 \sim \mathbf{U}\left(\mathbb{B}^P\right)$ in a SCISMM setup. We will prove by a mathematical induction that $\forall n \in \mathbb{N}, x^n \sim \mathbf{U}\left(\mathbb{B}^N\right)$. The base case is obvious according to the uniform repartition hypothesis.

Let us now suppose that the statement $x^n \sim \mathbf{U}\left(\mathbb{B}^N\right)$ holds for some n. For a given $k \in \mathbb{B}^N$, we denote by $\tilde{k_i} \in \mathbb{B}^N$ the vector defined by: $\forall i \in [\![0;\mathsf{N}-1]\!]$, if $k = (k_0, k_1, \ldots, k_i, \ldots, k_{\mathsf{N}-2}, k_{\mathsf{N}-1})$, then $\tilde{k_i} = \left(k_0, k_1, \ldots, \overline{k_i}, \ldots, k_{\mathsf{N}-2}, k_{\mathsf{N}-1}\right)$.

Let $E_{i,j}$ be the following events:

$$\forall (i,j) \in [\![0;\mathsf{N}-1]\!] \times [\![0;\mathsf{P}-1]\!], E_{i,j} =$$

$$S_p^{n+1} = i \wedge S_c^{n+1} = j \wedge m_j^{n+1} = k_i \wedge \left(x^n = k \vee x^n = \tilde{k_i}\right),$$

and $p = P\left(x^{n+1} = k\right)$. So,

$$p = P\left(\bigvee_{i\in[\![0;\mathsf{N}-1]\!],\, j\in[\![0;\mathsf{P}-1]\!]} E_{i,j}\right).$$

We now introduce the following notation: $P_1(i) = P\left(S_p^{n+1} = i\right)$, $P_2(j) = P\left(S_c^{n+1} = j\right)$, $P_3(i,j) = P\left(m_j^{n+1} = k_i\right)$, and $P_4(i) = P\left(x^n = k \vee x^n = \tilde{k}_i\right)$.

These four events are independent in SCISMM setup, thus:

$$p = \sum_{i\in[\![0;\mathsf{N}-1]\!],\, j\in[\![0;\mathsf{P}-1]\!]} P_1(i)P_2(i)P_3(i,j)P_4(i).$$

According to Proposition 3, $P\left(m_j^{n+1} = k_i\right) = \frac{1}{2}$. As the two events are incompatible:

$$P\left(x^n = k \vee x^n = \tilde{k}_i\right) = P\left(x^n = k\right) + P\left(x^n = \tilde{k}_i\right).$$

Then, by using the inductive hypothesis: $P\left(x^n = k\right) = \frac{1}{2^N}$, and $P\left(x^n = \tilde{k}_i\right) = \frac{1}{2^N}$.

Let S be defined by

$$S = \sum_{i\in[\![0;\mathsf{N}-1]\!],\, j\in[\![0;\mathsf{P}-1]\!]} P_1(i)P_2(j).$$

Then $p = 2 \times \frac{1}{2} \times \frac{1}{2^N} \times S = \frac{1}{2^N} \times S$.

S can now be evaluated:

$$\begin{array}{rcl} S & = & \sum_{i\in[\![0;\mathsf{N}-1]\!],\, j\in[\![0;\mathsf{P}-1]\!]} P_1(i)P_2(j) \\ & = & \sum_{i\in[\![0;\mathsf{N}-1]\!]} P_1(i) \times \sum_{j\in[\![0;\mathsf{P}-1]\!]} P_2(j). \end{array}$$

The set of events $\left\{S_p^{n+1} = i\right\}$ for $i \in [\![0; N-1]\!]$ and the set of events $\left\{S_c^{n+1} = j\right\}$ for $j \in [\![0; P-1]\!]$ are both a partition of the universe of possible, so $S = 1$.

Finally, $P\left(x^{n+1} = k\right) = \frac{1}{2^N}$, which leads to $x^{n+1} \sim \mathbf{U}\left(\mathbb{B}^N\right)$. This result is true $\forall n \in \mathbb{N}$, we thus have proven that the stego-content y is uniform in the set of possible stego-content, so $y \sim \mathbf{U}\left(\mathbb{B}^N\right)$ when $x \sim \mathbf{U}\left(\mathbb{B}^N\right)$. □

7 Topological model

In this section, we prove that SCISMM can be modeled as a discret dynamical system in a topological space. We will show in the next section that SCISMM is a case of topological chaos in the sense of Devaney.

7.1 Iteration Function and Phase Space

Let

$$\begin{array}{rl} F: & [\![0;\mathsf{N}-1]\!] \times \mathbb{B}^{\mathsf{N}} \times [\![0;\mathsf{P}-1]\!] \times \mathbb{B}^{\mathsf{P}} \longrightarrow \mathbb{B}^{\mathsf{N}} \\ & (k,x,\lambda,m) \longmapsto \left(\delta(k,j).x_j + \overline{\delta(k,j)}.m_\lambda\right)_{j\in[\![0;\mathsf{N}-1]\!]} \end{array}$$

where + and . are the boolean addition and product operations.

Consider the phase space $\mathcal{X}_2$ defined as follow:

$$\mathcal{X}_2 = \mathbb{S}_N \times \mathbb{B}^{\mathsf{N}} \times \mathbb{S}_P \times \mathbb{B}^{\mathsf{P}} \times \mathbb{S}_P,$$

where $\mathbb{S}_N$ and $\mathbb{S}_P$ are the sets introduced in Section 5.

We define the map $\mathcal{G}_{f_0} : \mathcal{X}_2 \longrightarrow \mathcal{X}_2$ by:

$$\mathcal{G}_{f_0}(S_p,x,S_c,m,S_m) =$$
$$(\sigma_N(S_p), F(i_N(S_p),x,i_P(S_c),m), \sigma_P(S_c), G_{f_0}(m,S_m), \sigma_P(S_m))$$

Then SCISMM can be described by the iterations of the following discret dynamical system:

$$\begin{cases} X^0 \in \mathcal{X}_2 \\ X^{k+1} = \mathcal{G}_{f_0}(X^k). \end{cases}$$

7.2 Cardinality of $\mathcal{X}_2$

By comparing $\mathcal{X}_2$ and $\mathcal{X}_1$, we have the following result.

Proposition 5. *The phase space $\mathcal{X}_2$ has, at least, the cardinality of the continuum.*

Proof. Let φ be the map defined as follow:

$$\begin{array}{rccc} \varphi: & \mathcal{X}_1 & \longrightarrow & \mathcal{X}_2 \\ & (S,x) & \longmapsto & (S,x,0,0,0) \end{array}$$

φ is injective. So the cardinality of $\mathcal{X}_2$ is greater than or equal to the cardinality of $\mathcal{X}_1$. And consequently $\mathcal{X}_2$ has at least the cardinality of the continuum. □

Remark 2. *This result is independent on the number of cells of the system.*

7.3 A New Distance on $\mathcal{X}_2$

We define a new distance on $\mathcal{X}_2$ as follow: $\forall X, \check{X} \in \mathcal{X}_2$, if $X = (S_p, x, S_c, m, S_m)$ and $\check{X} = (\check{S_p}, \check{x}, \check{S_c}, \check{m}, \check{S_m})$, then:

$$\begin{array}{rcl} d_2(X,\check{X}) & = & d_{\mathbb{B}^{\mathbb{N}}}(x,\check{x}) + d_{\mathbb{B}^{\mathbb{P}}}(m,\check{m}) \\ & + & d_{\mathbb{S}_N}(S_p,\check{S_p}) + d_{\mathbb{S}_P}(S_c,\check{S_c}) + d_{\mathbb{S}_P}(S_m,\check{S_m}), \end{array}$$

where $d_{\mathbb{B}^{\mathbb{N}}}$, $d_{\mathbb{B}^{\mathbb{P}}}$, $d_{\mathbb{S}_N}$, and $d_{\mathbb{S}_P}$ are the same distances than in Definition 13.

7.4 Continuity of SCISMM

To prove that SCISMM is another example of topological chaos in the sense of Devaney, $\mathcal{G}_{f_0}$ must be continuous on the metric space $(\mathcal{X}_2, d_2)$.

Proposition 6. *$\mathcal{G}_{f_0}$ is a continuous function on $(\mathcal{X}_2, d_2)$.*

Proof. We use the sequential continuity.

Let $((S_p)^n, x^n, (S_c)^n, m^n, (S_m)^n)_{n\in\mathbb{N}}$ be a sequence of the phase space $\mathcal{X}_2$, which converges to (S_p, x, S_c, m, S_m). We will prove that $(\mathcal{G}_{f_0}((S_p)^n, x^n, (S_c)^n, m^n, (S_m)^n))_{n\in\mathbb{N}}$ converges to $\mathcal{G}_{f_0}(S_p, x, S_c, m, S_m)$. Let us recall that for all n, $(S_p)^n$, $(S_c)^n$ and $(S_m)^n$ are strategies, thus we consider a sequence of strategies (*i.e.*, a sequence of sequences).

As $d_2(((S_p)^n, x^n, (S_c)^n, m^n, (S_m)^n), (S_p, x, S_c, m, S_m))$ converges to 0, each distance $d_{\mathbb{B}^{\mathbb{N}}}(x^n, x)$, $d_{\mathbb{B}^{\mathbb{P}}}(m^n, m)$, $d_{\mathbb{S}_N}((S_p)^n, S_p)$, $d_{\mathbb{S}_P}((S_c)^n, S_c)$, and $d_{\mathbb{S}_P}((S_m)^n, S_m)$ converges to 0. But $d_{\mathbb{B}^{\mathbb{N}}}(x^n, x)$ and $d_{\mathbb{B}^{\mathbb{P}}}(m^n, m)$ are integers, so $\exists n_0 \in \mathbb{N}, \forall n \geqslant n_0, d_{\mathbb{B}^{\mathbb{N}}}(x^n, x) = 0$ and $\exists n_1 \in \mathbb{N}, \forall n \geqslant n_1, d_{\mathbb{B}^{\mathbb{P}}}(m^n, m) = 0$.

Let $n_3 = Max(n_0, n_1)$. In other words, there exists a threshold $n_3 \in \mathbb{N}$ after which no cell will change its state: $\exists n_3 \in \mathbb{N}, n \geqslant n_3 \Longrightarrow (x^n = x) \wedge (m^n = m)$.

In addition, $d_{\mathbb{S}_N}((S_p)^n, S_p) \longrightarrow 0$, $d_{\mathbb{S}_P}((S_c)^n, S_c) \longrightarrow 0$, and $d_{\mathbb{S}_P}((S_m)^n, S_m) \longrightarrow 0$, so $\exists n_4, n_5, n_6 \in \mathbb{N}$,

- $\forall n \geqslant n_4, d_{\mathbb{S}_N}((S_p)^n, S_p) < 10^{-1}$,
- $\forall n \geqslant n_5, d_{\mathbb{S}_P}((S_c)^n, S_c) < 10^{-1}$,
- $\forall n \geqslant n_6, d_{\mathbb{S}_P}((S_m)^n, S_m) < 10^{-1}$.

Let $n_7 = Max(n_4, n_5, n_6)$. For $n \geqslant n_7$, all the strategies $(S_p)^n$, $(S_c)^n$, and $(S_m)^n$ have the same first term, which are respectively $(S_p)_0$,$(S_c)_0$ and $(S_m)_0$:$\forall n \geqslant n_7$,

$$((S_p)^n_0 = (S_p)_0) \wedge ((S_c)^n_0 = (S_c)_0) \wedge ((S_m)^n_0 = (S_m)_0).$$

Let $n_8 = Max(n_3, n_7)$. After the n_8-th term, states of x^n and x on the one hand, and m^n and m on the other hand, are identical. Additionally, strategies $(S_p)^n$ and S_p, $(S_c)^n$ and S_c, and $(S_m)^n$ and S_m start with the same first term.

Consequently, states of $\mathcal{G}_{f_0}((S_p)^n, x^n, (S_c)^n, m^n, (S_m)^n)$ and $\mathcal{G}_{f_0}(S_p, x, S_c, m, S_m)$ are equal, so, after the $(n_8)^{th}$ term, the distance d_2 between these two points is strictly smaller than 3.10^{-1}, so strictly smaller than 1.

We now prove that the distance between $(\mathcal{G}_{f_0}((S_p)^n, x^n, (S_c)^n, m^n, (S_m)^n))$ and $(\mathcal{G}_{f_0}(S_p, x, S_c, m, S_m))$ is convergent to 0. Let $\varepsilon > 0$.

- If $\varepsilon \geqslant 1$, we have seen that distance between $\mathcal{G}_{f_0}((S_p)^n, x^n, (S_c)^n, m^n, (S_m)^n)$ and $\mathcal{G}_{f_0}(S_p, x, S_c, m, S_m)$ is strictly less than 1 after the $(n_8)^{th}$ term (same state).

- If $\varepsilon < 1$, then $\exists k \in \mathbb{N}, 10^{-k} \geqslant \frac{\varepsilon}{3} \geqslant 10^{-(k+1)}$. As $d_{\mathbb{S}_N}((S_p)^n, S_p)$, $d_{\mathbb{S}_P}((S_c)^n, S_c)$ and $d_{\mathbb{S}_P}((S_m)^n, S_m)$ converges to 0, we have:
  - $\exists n_9 \in \mathbb{N}, \forall n \geqslant n_9, d_{\mathbb{S}_N}((S_p)^n, S_p) < 10^{-(k+2)}$,
  - $\exists n_{10} \in \mathbb{N}, \forall n \geqslant n_{10}, d_{\mathbb{S}_P}((S_c)^n, S_c) < 10^{-(k+2)}$,
  - $\exists n_{11} \in \mathbb{N}, \forall n \geqslant n_{11}, d_{\mathbb{S}_P}((S_m)^n, S_m) < 10^{-(k+2)}$.

  Let $n_{12} = Max(n_9, n_{10}, n_{11})$ thus after n_{12}, the $k+2$ first terms of $(S_p)^n$ and S_p, $(S_c)^n$ and S_c, and $(S_m)^n$ and S_m, are equal.

As a consequence, the $k+1$ first entries of the strategies of $\mathcal{G}_{f_0}((S_p)^n, x^n, (S_c)^n, m^n, (S_m)^n)$ and $\mathcal{G}_{f_0}(S_p, x, S_c, m, S_m)$ are the same (due to the shift of strategies) and following the definition of $d_{\mathbb{S}_N}$ and $d_{\mathbb{S}_P}$:

$$d_2\left(\mathcal{G}_{f_0}((S_p)^n, x^n, (S_c)^n, m^n, (S_m)^n); \mathcal{G}_{f_0}(S_p, x, S_c, m, S_m)\right)$$

is equal to :

$$d_{\mathbb{S}_N}((S_p)^n, S_p) + d_{\mathbb{S}_P}((S_c)^n, S_c) + d_{\mathbb{S}_P}((S_m)^n, S_m)$$

which is smaller than $3.10^{-(k+1)} \leqslant 3.\frac{\varepsilon}{3} = \varepsilon$.

Let $N_0 = max(n_8, n_{12})$. We can claim that

$$\forall \varepsilon > 0, \exists N_0 \in \mathbb{N}, \forall n \geqslant N_0,$$

$$d_2\left(\mathcal{G}_{f_0}((S_p)^n, x^n, (S_c)^n, m^n, (S_m)^n); \mathcal{G}_{f_0}(S_p, x, S_c, m, S_m)\right) \leqslant \varepsilon.$$

$\mathcal{G}_{f_0}$ is consequently continuous on $(\mathcal{X}_2, d_2)$. □

8 SCISMM is chaotic

To prove that we are in the framework of Devaney's topological chaos, we have to check the regularity, transitivity, and sensitivity conditions.

8.1 Regularity

Proposition 7. *Periodic points of $\mathcal{G}_{f_0}$ are dense in $\mathcal{X}_2$.*

Proof. Let $(\check{S_p}, \check{x}, \check{S_c}, \check{m}, \check{S_m}) \in \mathcal{X}_2$ and $\varepsilon > 0$. We are looking for a periodic point $(\widetilde{S_p}, \widetilde{x}, \widetilde{S_c}, \widetilde{m}, \widetilde{S_m})$ satisfying $d_2((\check{S_p}, \check{x}, \check{S_c}, \check{m}, \check{S_m}); (\widetilde{S_p}, \widetilde{x}, \widetilde{S_c}, \widetilde{m}, \widetilde{S_m})) < \varepsilon$.

As ε can be strictly lesser than 1, we must choose $\widetilde{x} = \check{x}$ and $\widetilde{m} = \check{m}$. Let us define $k_0(\varepsilon) = \lfloor -log_{10}(\frac{\varepsilon}{3}) \rfloor + 1$ and consider the set: $\mathcal{S}_{\check{S_p}, \check{S_c}, \check{S_m}, k_0(\varepsilon)} = \Big\{ S \in \mathbb{S}_N \times \mathbb{S}_P \times \mathbb{S}_P / ((S_p)^k = \check{S_p}^k) \wedge ((S_c)^k = \check{S_c}^k)) \wedge ((S_m)^k = \check{S_m}^k)), \forall k \leqslant k_0(\varepsilon) \Big\}$.

Then, $\forall (S_p, S_c, S_m) \in \mathcal{S}_{\check{S_p}, \check{S_c}, \check{S_m}, k_0(\varepsilon)}$, $d_2((S_p, \check{x}, S_c, \check{m}, S_m); (\check{S_p}, \check{x}, \check{S_c}, \check{m}, \check{S_m})) < 3.\frac{\varepsilon}{3} = \varepsilon$. It remains to choose $(\widetilde{S_p}, \widetilde{S_p}, \widetilde{S_p}) \in \mathcal{S}_{\check{S_p}, \check{S_c}, \check{S_m}, k_0(\varepsilon)}$ such that $(\widetilde{S_p}, \widetilde{x}, \widetilde{S_c}, \widetilde{m}, \widetilde{S_m}) = (\widetilde{S_p}, \check{x}, \widetilde{S_c}, \check{m}, \widetilde{S_m})$ is a periodic point for $\mathcal{G}_{f_0}$.

Let $\mathcal{J} = \{ i \in [\![0; \mathsf{N}-1]\!] / x_i \neq \check{x}_i, \text{ where } (S_p, x, S_c, m, S_m) = \mathcal{G}_{f_0}^{k_0}(\check{S_p}, \check{x}, \check{S_c}, \check{m}, \check{S_m}) \Big\}$, $\lambda = card(\mathcal{J})$, and $j_0 < j_1 < ... < j_{\lambda-1}$ the elements of $\mathcal{J}$.

1. Let us firstly build three strategies: S_p^*, S_c^*, and S_m^*, as follows.
   (a) $(S_p^*)^k = \check{S_p}^k$, $(S_c^*)^k = \check{S_c}^k$, and $(S_m^*)^k = \check{S_m}^k$, if $k \leqslant k_0(\varepsilon)$.
   (b) Let us now explain how to replace $\check{x}_{j_q}$, $\forall q \in [\![0; \lambda-1]\!]$:
   First of all, we must replace $\check{x}_{j_0}$:
      i. If $\exists \lambda_0 \in [\![0; \mathsf{P}-1]\!] / \check{x}_{j_0} = m_{\lambda_0}$, then we can choose $(S_p^*)^{k_0+1} = j_0$, $(S_c^*)^{k_0+1} = \lambda_0$, $(S_m^*)^{k_0+1} = \lambda_0$, and so I_{j_0} will be equal to 1.

ii. If such a λ_0 does not exist, we choose:
$(S_p^*)^{k_0+1} = j_0$, $(S_c^*)^{k_0+1} = 0$, $(S_m^*)^{k_0+1} = 0$,
$(S_p^*)^{k_0+2} = j_0$, $(S_c^*)^{k_0+2} = 0$, $(S_m^*)^{k_0+2} = 0$,
and $I_{j_0} = 2$.

All of the $\check{x}_{j_q}$ are replaced similarly. The other terms of S_p^*, S_c^*, and S_m^* are constructed identically, and the values of I_{j_q} are defined in the same way.
Let $\gamma = \sum_{q=0}^{\lambda-1} I_{j_q}$.

(c) Finally, let $(S_p^*)^k = (S_p^*)^j$, $(S_c^*)^k = (S_c^*)^j$, and $(S_m^*)^k = (S_m^*)^j$, where $j \leqslant k_0(\varepsilon)+\gamma$ is satisfying $j \equiv k \ [\mathrm{mod}\ (k_0(\varepsilon)+\gamma)]$, if $k > k_0(\varepsilon)+\gamma$.

So, $\mathcal{G}_{f_0}^{k_0(\varepsilon)+\gamma}(S_p^*, \check{x}, S_c^*, \check{m}, S_m^*) = (S_p^*, \check{x}, S_c^*, m, S_m^*)$. Let $\mathcal{K} = \{i \in [\![0; \mathsf{P}-1]\!] / m_i \neq \check{m}_i, \text{ where } \mathcal{G}_{f_0}^{k_0(\varepsilon)+\gamma}(S_p^*, \check{x}, S_c^*, \check{m}, S_m^*) = (S_p^*, \check{x}, S_c^*, m, S_m^*)\Big\}$,
$\mu = card(\mathcal{K})$, and $r_0 < r_1 < ... < r_{\mu-1}$ the elements of $\mathcal{K}$.

2. Let us now build the strategies $\widetilde{S_p}$, $\widetilde{S_c}$, $\widetilde{S_m}$.

(a) Firstly, let $\widetilde{S_p}^k = (S_p^*)^k$, $\widetilde{S_c}^k = (S_c^*)^k$, and $\widetilde{S_m}^k = (S_m^*)^k$, if $k \leqslant k_0(\varepsilon)+\gamma$.

(b) How to replace $\check{m}_{r_q}, \forall q \in [\![0; \mu-1]\!]$:

First of all, let us explain how to replace $\check{m}_{r_0}$:

i. If $\exists \mu_0 \in [\![0; \mathsf{N}-1]\!] / \check{x}_{\mu_0} = m_{r_0}$, then we can choose $\widetilde{S_p}^{k_0+\gamma+1} = \mu_0$, $\widetilde{S_c}^{k_0+\gamma+1} = r_0$, $\widetilde{S_m}^{k_0+\gamma+1} = r_0$.
In that situation, we define $J_{r_0} = 1$.

ii. If such a μ_0 does not exist, then we can choose:
$\widetilde{S_p}^{k_0+\gamma+1} = 0$, $\widetilde{S_c}^{k_0+\gamma+1} = r_0$, $\widetilde{S_m}^{k_0+\gamma+1} = r_0$,
$\widetilde{S_p}^{k_0+\gamma+2} = 0$, $\widetilde{S_c}^{k_0+\gamma+2} = r_0$, $\widetilde{S_m}^{k_0+\gamma+2} = 0$,
$\widetilde{S_p}^{k_0+\gamma+3} = 0$, $\widetilde{S_c}^{k_0+\gamma+3} = r_0$, $\widetilde{S_m}^{k_0+\gamma+3} = 0$.
Let $J_{r_0} = 3$.
Then the other $\check{m}_{r_q}$ are replaced as previously, the other terms of $\widetilde{S_p}$, $\widetilde{S_c}$, and $\widetilde{S_m}$ are constructed in the same way, and the values of J_{r_q} are defined similarly.
Let $\alpha = \sum_{q=0}^{\mu-1} J_{r_q}$.

(c) Finally, let $\widetilde{S_p}^k = \widetilde{S_p}^j$, $\widetilde{S_c}^k = \widetilde{S_c}^j$, and $\widetilde{S_m}^k = \widetilde{S_m}^j$ where $j \leqslant k_0(\varepsilon)+\gamma+\alpha$ is satisfying $j \equiv k \ [\mathrm{mod}\ (k_0(\varepsilon)+\gamma+\alpha)]$, if $k > k_0(\varepsilon)+\gamma+\alpha$.

So, $\mathcal{G}_{f_0}^{k_0(\varepsilon)+\gamma+\alpha}(\widetilde{S_p}, \check{x}, \widetilde{S_c}, \check{m}, \widetilde{S_m}) = (\widetilde{S_p}, \check{x}, \widetilde{S_c}, \check{m}, \widetilde{S_m})$

Then, $(\widetilde{S_p}, \widetilde{S_c}, \widetilde{S_m}) \in \mathcal{S}_{\check{S_p}, \check{S_c}, \check{S_m}, k_0(\varepsilon)}$ defined as previous is such that $(\widetilde{S_m}, \check{x}, \widetilde{S_m}, \check{m}, \widetilde{S_m})$ is a periodic point, of period $k_0(\varepsilon)+\gamma+\alpha$, which is $\varepsilon-$close to $(\check{S_p}, \check{x}, \check{S_c}, \check{m}, \check{S_m})$.

As a conclusion, $(\mathcal{X}_2, \mathcal{G}_{f_0})$ is regular. □

8.2 Transitivity

Proposition 8. *$(\mathcal{X}_2, \mathcal{G}_{f_0})$ is topologically transitive.*

Proof. Let us define $\mathcal{X} : \mathcal{X}_2 \to \mathbb{B}^{\mathsf{N}}$, such that $\mathcal{X}(S_p, x, S_c, m, S_m) = x$ and $\mathcal{M} : \mathcal{X}_2 \to \mathbb{B}^{\mathsf{P}}$, such that $\mathcal{M}(S_p, x, S_c, m, S_m) = m$. Let $\mathcal{B}_A = \mathcal{B}(X_A, r_A)$ and $\mathcal{B}_B = \mathcal{B}(X_B, r_B)$ be two open balls of $\mathcal{X}_2$, with $X_A = ((S_p)_A, x_A, (S_c)_A, m_A, (S_m)_A)$ and $X_B = ((S_p)_B, x_B, (S_c)_B, m_B, (S_m)_B)$. We are looking for $\widetilde{X} = (\widetilde{S_p}, \widetilde{x}, \widetilde{S_c}, \widetilde{m}, \widetilde{S_m})$ in $\mathcal{B}_A$ such that $\exists n_0 \in \mathbb{N}, \mathcal{G}_{f_0}^{n_0}(\widetilde{X}) \in \mathcal{B}_B$.

$\widetilde{X}$ must be in $\mathcal{B}_A$ and r_A can be strictly lesser than 1, so $\widetilde{x} = x_A$ and $\widetilde{m} = m_A$. Let $k_0 = \lfloor -\log_{10}(\frac{r_A}{3}) + 1 \rfloor$. Let us notice $\mathcal{S}_{X_A, k_0} = \big\{(S_p, S_c, S_m) \in \mathbb{S}_{\mathsf{N}} \times (\mathbb{S}_{\mathsf{P}})^2 / \forall k \leqslant k_0, \ (S_p^k = (S_p)_A^k) \wedge (S_c^k = (S_c)_A^k) \wedge (S_m^k = (S_m)_A^k))\big\}$.
Then $\forall (S_p, S_c, S_m) \in \mathcal{S}_{X_A, k_0}, (S_p, \widetilde{x}, S_c, \widetilde{m}, S_m) \in \mathcal{B}_A$.

Let $\mathcal{J} = \{i \in [\![0, \mathsf{N}-1]\!] / \check{x}_i \neq \mathcal{X}(X_B)_i, \text{ where } (\check{S}_p, \check{x}, \check{S}_c, \check{m}, \check{S}_m) = \mathcal{G}_{f_0}^{k_0}(X_A)\}$, $\lambda = card(\mathcal{J})$, and $j_0 < j_1 < ... < j_{\lambda-1}$ the elements of $\mathcal{J}$.

1. Let us firstly build three strategies: S_p^*, S_c^*, and S_m^* as follows.
   (a) $(S_p^*)^k = (S_p)_A^k$, $(S_c^*)^k = (S_c)_A^k$, and $(S_m^*)^k = (S_m)_A^k$, if $k \leqslant k_0$.
   (b) Let us now explain how to replace $\mathcal{X}(X_B)_{j_q}$, $\forall q \in [\![0; \lambda-1]\!]$:
   First of all, we must replace $\mathcal{X}(X_B)_{j_0}$:
      i. If $\exists \lambda_0 \in [\![0; \mathsf{P}-1]\!] / \mathcal{X}(X_B)_{j_0} = \check{m}_{\lambda_0}$, then we can choose $(S_p^*)^{k_0+1} = j_0$, $(S_c^*)^{k_0+1} = \lambda_0$, $(S_m^*)^{k_0+1} = \lambda_0$, and so I_{j_0} will be equal to 1.
      ii. If such a λ_0 does not exist, we choose:
      $(S_p^*)^{k_0+1} = j_0$, $(S_c^*)^{k_0+1} = 0$, $(S_m^*)^{k_0+1} = 0$,
      $(S_p^*)^{k_0+2} = j_0$, $(S_c^*)^{k_0+2} = 0$, $(S_m^*)^{k_0+2} = 0$
      and so let us notice $I_{j_0} = 2$.

      All of the $\mathcal{X}(X_B)_{j_q}$ are replaced similarly. The other terms of S_p^*, S_c^*, and S_m^* are constructed identically, and the values of I_{j_q} are defined on the same way.
      Let $\gamma = \sum_{q=0}^{\lambda-1} I_{j_q}$.
   (c) $(S_p^*)^k = (S_p^*)^j$, $(S_c^*)^k = (S_c^*)^j$ and $(S_m^*)^k = (S_m^*)^j$ where $j \leqslant k_0 + \gamma$ is satisfying $j \equiv k \ [\mathrm{mod}\ (k_0+\gamma)]$, if $k > k_0 + \gamma$.

   So, $\mathcal{G}_{f_0}^{k_0+\gamma}((S_p^*, x_A, S_c^*, m_A, S_m^*)) = (S_p^*, x_B, S_c^*, m, S_m^*)$
   Let $\mathcal{K} = \{i \in [\![0; \mathsf{P}-1]\!] / m_i \neq \mathcal{M}(X_B)_i, \text{ where } (S_p^*, x_B, S_c^*, m, S_m^*) = \mathcal{G}_{f_0}^{k_0+\gamma}((S_p^*, x_A, S_c^*, m_A, S_m^*))\}$,
   $\mu = card(\mathcal{K})$ and $r_0 < r_1 < ... < r_{\mu-1}$ the elements of $\mathcal{K}$.
2. Let us secondly build three other strategies: $\widetilde{S_p}$, $\widetilde{S_c}$, $\widetilde{S_m}$ as follows.
   (a) $\widetilde{S_p}^k = (S_p^*)^k$, $\widetilde{S_c}^k = (S_c^*)^k$, and $\widetilde{S_m}^k = (S_m^*)^k$, if $k \leqslant k_0 + \gamma$.
   (b) Let us now explain how to replace $\mathcal{M}(X_B)_{r_q}, \forall q \in [\![0; \mu-1]\!]$:
   First of all, we must replace $\mathcal{M}(X_B)_{r_0}$:
      i. If $\exists \mu_0 \in [\![0; \mathsf{N}-1]\!] / \mathcal{M}(X_B)_{r_0} = (x_B)_{\mu_0}$, then we can choose $\widetilde{S_p}^{k_0+\gamma+1} = \mu_0$, $\widetilde{S_c}^{k_0+\gamma+1} = r_0$, $\widetilde{S_m}^{k_0+\gamma+1} = r_0$, and J_{r_0} will be equal to 1.
      ii. If such a μ_0 does not exist, we choose: $\widetilde{S_p}^{k_0+\gamma+1} = 0$, $\widetilde{S_c}^{k_0+\gamma+1} = r_0$, $\widetilde{S_m}^{k_0+\gamma+1} = r_0$,
      $\widetilde{S_p}^{k_0+\gamma+2} = 0$, $\widetilde{S_c}^{k_0+\gamma+2} = r_0$, $\widetilde{S_m}^{k_0+\gamma+2} = 0$,
      $\widetilde{S_p}^{k_0+\gamma+3} = 0$, $\widetilde{S_c}^{k_0+\gamma+3} = r_0$, $\widetilde{S_m}^{k_0+\gamma+3} = 0$,
      and so let us notice $J_{r_0} = 3$.

      All the $\mathcal{M}(X_B)_{r_q}$ are replaced similarly. The other terms of $\widetilde{S_p}$, $\widetilde{S_c}$, and $\widetilde{S_m}$ are constructed identically, and the values of J_{r_q} are defined on the same way.
      Let $\alpha = \sum_{q=0}^{\mu-1} J_{r_q}$.
   (c) $\forall k \in \mathbb{N}^*, \widetilde{S_p}^{k_0+\gamma+\alpha+k} = (S_p)_B^k$, $\widetilde{S_c}^{k_0+\gamma+\alpha+k} = (S_c)_B^k$, and $\widetilde{S_m}^{k_0+\gamma+\alpha+k} = (S_m)_B^k$.

So, $\mathcal{G}_{f_0}^{k_0+\gamma+\alpha}(\widetilde{S_p}, x_A, \widetilde{S_c}, m_A, \widetilde{S_m}) = X_B$, with $(\widetilde{S_p}, \widetilde{S_c}, \widetilde{S_m}) \in \mathcal{S}_{X_A, k_0}$. Then $\widetilde{X} = (\widetilde{S_p}, x_A, \widetilde{S_c}, m_A, \widetilde{S_m}) \in \mathcal{X}_2$ is such that $\widetilde{X} \in \mathcal{B}_A$ and $\mathcal{G}_{f_0}^{k_0+\gamma+\alpha}(\widetilde{X}) \in \mathcal{B}_B$. Finally we have proven the result. □

8.3 Sensitivity on Initial Conditions

Proposition 9. *$(\mathcal{X}_2, \mathcal{G}_{f_0})$ has sensitive dependence on initial conditions.*

Proof. $\mathcal{G}_{f_0}$ is regular and transitive. Due to Theorem 1, $\mathcal{G}_{f_0}$ is sensitive. □

8.4 Devaney's topological chaos

In conclusion, $(\mathcal{X}_2, \mathcal{G}_{f_0})$ is topologically transitive, regular, and has sensitive dependence on initial conditions. Then we have the result.

Theorem 3. *$\mathcal{G}_{f_0}$ is a chaotic map on $(\mathcal{X}_2, d_2)$ in the sense of Devaney.*

So we can claim that:

Theorem 4. *SCISMM is topologically-secure.*

9 Conclusion

In this research work, a new information hiding scheme has been introduced. It is topologically-secure and stego-secure, and thus is able to withstand attacks in Watermark-Only Attack (WOA) and Constant-Message Attack (CMA) setups. These results have been obtained after having studied the topological behavior of this data hiding scheme. To the best of our knowledge, this algorithm is the third scheme that has been proven to be secure, according to the information hiding security field.

In future work, we intend to study the robustness of this scheme, and to compare it with the two other secure algorithms. Additionally, we will investigate the topological properties of our scheme, to see whether it is secure in KOA and KMA setups.

References

[1] Jacques Bahi and Christophe Guyeux. Hash functions using chaotic iterations. *Journal of Algorithms & Computational Technology*, 4(2):167–181, 2010.

[2] Jacques Bahi and Christophe Guyeux. A new chaos-based watermarking algorithm. In *SECRYPT 2010, International conference on security and cryptography*, Athens, Greece, 2010. To appear.

[3] Jacques M. Bahi and Christophe Guyeux. A chaos-based approach for information hiding security. arXiv N^o 0034939, April 2010.

[4] J. Banks, J. Brooks, G. Cairns, and P. Stacey. On devaney's definition of chaos. *Amer. Math. Monthly*, 99:332–334, 1992.

[5] Mauro Barni, Franco Bartolini, and Teddy Furon. A general framework for robust watermarking security. *Signal Processing*, 83(10):2069–2084, 2003. Special issue on Security of Data Hiding Technologies, invited paper.

[6] Richard Bergmair and Stefan Katzenbeisser. Content-aware steganography: About lazy prisoners and narrow-minded wardens. In Camenisch et al. [9], pages 109–123.

[7] Maria Bras-Amorós and Josep Domingo-Ferrer. On overlappings of digitized straight lines and shared steganographic file systems. *Transactions on Data Privacy*, 1(3):131–139, 2008.

[8] Christian Cachin. An information-theoretic model for steganography. *Information and Computation*, 192:41 – 56, 2004.

[9] Jan Camenisch, Christian S. Collberg, Neil F. Johnson, and Phil Sallee, editors. *Information Hiding, 8th International Workshop, IH 2006, Alexandria, VA, USA, July 10-12, 2006. Revised Selcted Papers*, volume 4437 of *Lecture Notes in Computer Science*. Springer, 2007.

[10] Francois Cayre, Caroline Fontaine, and Teddy Furon. Kerckhoffs-based embedding security classes for woa data hiding. *IEEE Transactions on Information Forensics and Security*, 3(1):1–15, 2008.

[11] Franois Cayre, Caroline Fontaine, and Teddy Furon. Watermarking security: theory and practice. *IEEE Transactions on Signal Processing*, 53(10):3976–3987, 2005.

[12] Robert L. Devaney. *An Introduction to Chaotic Dynamical Systems*. Addison-Wesley, Redwood City, CA, 2nd edition, 1989.

[13] Josep Domingo-Ferrer and Maria Bras-Amorós. A shared steganographic file system with error correction. In Vicenç Torra and Yasuo Narukawa, editors, *MDAI*, volume 5285 of *Lecture Notes in Computer Science*, pages 227–238. Springer, 2008.

[14] T. Furon. Security analysis, 2002. European Project IST-1999-10987 CERTIMARK, Deliverable D.5.5.

[15] Christophe Guyeux, Nicolas Friot, and Jacques Bahi. Chaotic iterations versus spread-spectrum: chaos and stego security. In *IIH-MSP'10, 6-th Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, pages 208–211, Darmstadt, Germany, October 2010.

[16] T. Kalker. Considerations on watermarking security. pages 201–206, 2001.

[17] Stefan Katzenbeisser and Jana Dittmann. Malicious attacks on media authentication schemes based on invertible watermarks. In Edward J. Delp and Ping Wah Wong, editors, *Security, Steganography, and Watermarking of Multimedia Contents*, volume 5306 of *Proceedings of SPIE*, pages 838–847. SPIE, 2004.

[18] Andrew D. Ker. Batch steganography and pooled steganalysis. In Camenisch et al. [9], pages 265–281.

[19] Thomas Mittelholzer. An information-theoretic approach to steganography and watermarking. In Andreas Pfitzmann, editor, *Information Hiding*, volume 1768 of *Lecture Notes in Computer Science*, pages 1–16, Dresden, Germany, September 29 - October 1. 1999. Springer.

[20] Luis Perez-Freire, F. Prez-gonzalez, and Pedro Comesaa. Secret dither estimation in lattice-quantization data hiding: A set-membership approach. In Edward J. Delp and Ping W. Wong, editors, *Security, Steganography, and Watermarking of Multimedia Contents*, San Jose, California, USA, January 2006. SPIE.

[21] Claude E. Shannon. Communication theory of secrecy systems. *Bell Systems Technical Journal*, 28:656–715, 1949.

[22] Li Shujun, Li Qi, Li Wenmin, Mou Xuanqin, and Cai Yuanlong. Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding. *Proceedings of the 8th IMA International Conference on Cryptography and Coding*, 1:205–221, 2001.

[23] Gustavus J. Simmons. The prisoners' problem and the subliminal channel. In *Advances in Cryptology, Proc. CRYPTO'83*, pages 51–67, 1984.